Configureer 802.11w Management Frame Protection op WLC

Inhoud

Inleiding

Dit document beschrijft informatie over de bescherming van het IEEE 802.11w-beheerframe en de configuratie ervan op de Cisco Wireless LAN-controller (WLC).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Cisco WLC die code 7.6 of hoger uitvoert.

Gebruikte componenten

De informatie in dit document is gebaseerd op WLC 5508 die code 7.6 in werking stelt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De 802.11w-standaard heeft als doel controle- en beheerframes en een set robuuste beheerframes te beschermen tegen vervalsing en terugspelen. De beschermde kadertypes omvatten Ontkoppeling, Deauthenticatie, en de Robuuste kaders van de Actie zoals:

- Spectrumbeheer
- Quality-of-Service (QoS)
- Block back

- Radiometing
- Fast Basic Service Set (BSS) - overgang

802.11w versleutelt de frames niet, maar beschermt de beheerframes. Het zorgt ervoor dat de boodschappen afkomstig zijn van legitieme bronnen. Om dat te doen, moet je een Message Integrity Check (MIC) element toevoegen. 802.11w heeft een nieuwe sleutel geïntroduceerd, de zogenaamde Integrity Group Temporal Key (IGTK), die wordt gebruikt om broadcast/multicast robuuste beheerframes te beveiligen. Dit is afgeleid als deel van het vierwegs sleutelhandshake-proces dat wordt gebruikt met Wireless Protected Access (WPA). Dit maakt dot1x/Pre-Shared Key (PSK) een vereiste wanneer u 802.11w moet gebruiken. Het kan niet worden gebruikt met open/webauth Service Set Identifier (SSID).

Wanneer over de bescherming van het beheerframe wordt onderhandeld, worden de GTK- en IGTK-waarden door het access point (AP) versleuteld in het EAPOL-sleutelframe dat in bericht 3 van de 4-voudige handdruk wordt geleverd. Als het toegangspunt later de GTK wijzigt, worden de nieuwe GTK en IGTK met behulp van de Group Key Handshake naar de client verzonden. Het voegt een MIC toe die wordt berekend met behulp van de IGTK-toets.

Management-MIC-informatie-element (MMIE)

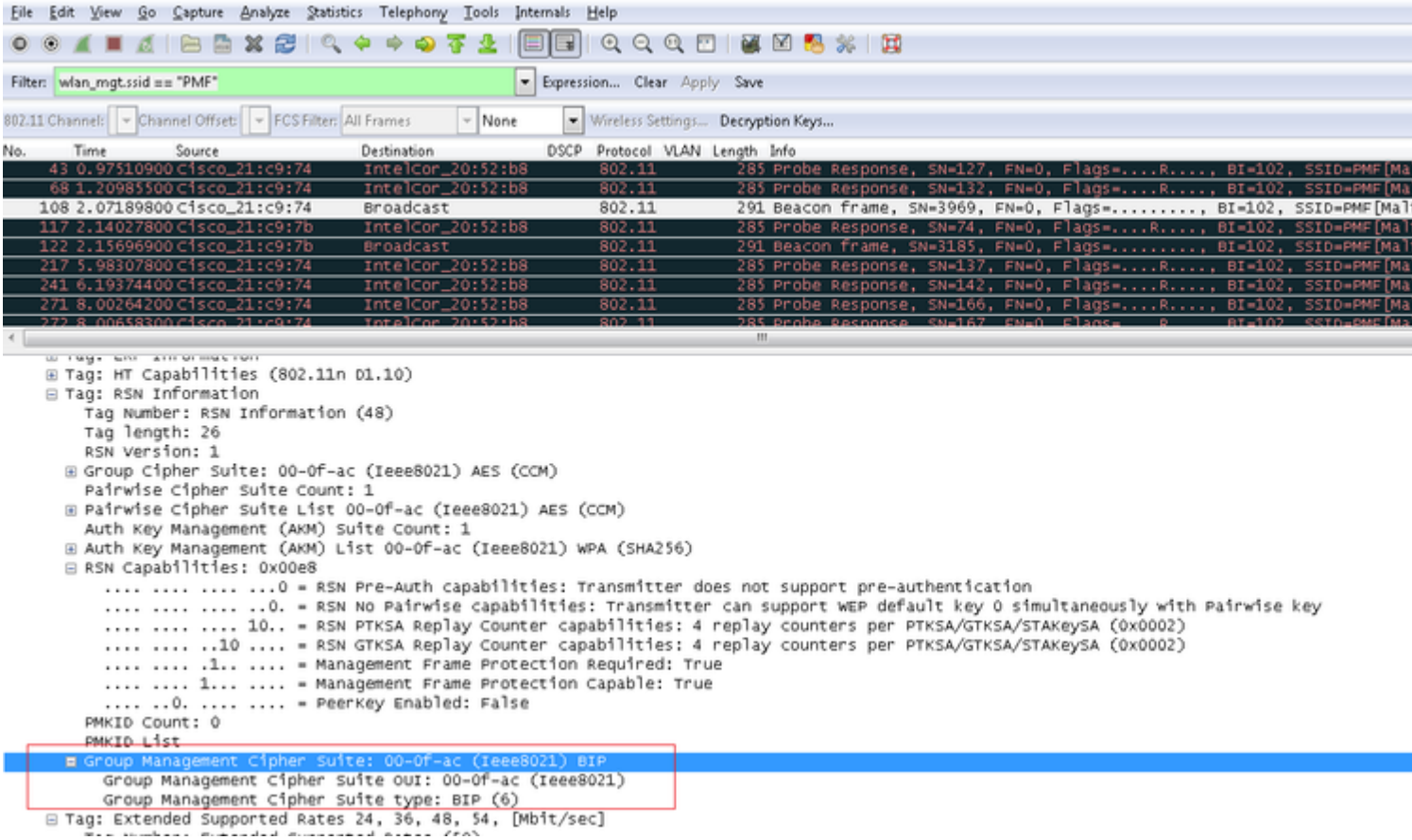
802.11w introduceert een nieuw informatie-element, het Management MIC-informatie-element. De header-indeling is beschikbaar zoals in de afbeelding.

De belangrijkste punten van zorg zijn **element ID** en **MIC**. De element-ID voor MMIE is 0x4c en het is een nuttige identificatie wanneer je de draadloze opnamen analyseert.

> **Opmerking**: MIC - Het bevat de berichtintegriteitscode berekend over het beheerframe. Het is belangrijk om op te merken dat dit wordt toegevoegd aan het toegangspunt. De doelclient berekent vervolgens de MIC voor het frame opnieuw en vergelijkt deze met wat door het toegangspunt is verzonden. Als de waarden verschillend zijn, wordt dit als ongeldig kader verworpen.

Wijzigingen in RSN IE

Robust Security Network Information Element (RSN IE) specificeert de beveiligingsparameters die worden ondersteund door het toegangspunt. De 802.11w introduceert een groepsbeheerprogrammeerkeuzeschakelaar in RSN IE die de programmeerkeuzeschakelaar bevat die door het toegangspunt wordt gebruikt om robuuste beheerframes voor broadcast/multicast te beveiligen. Dit is de beste manier om te weten of een AP 802.11w doet of niet. Dit kan ook worden geverifieerd zoals in de afbeelding.

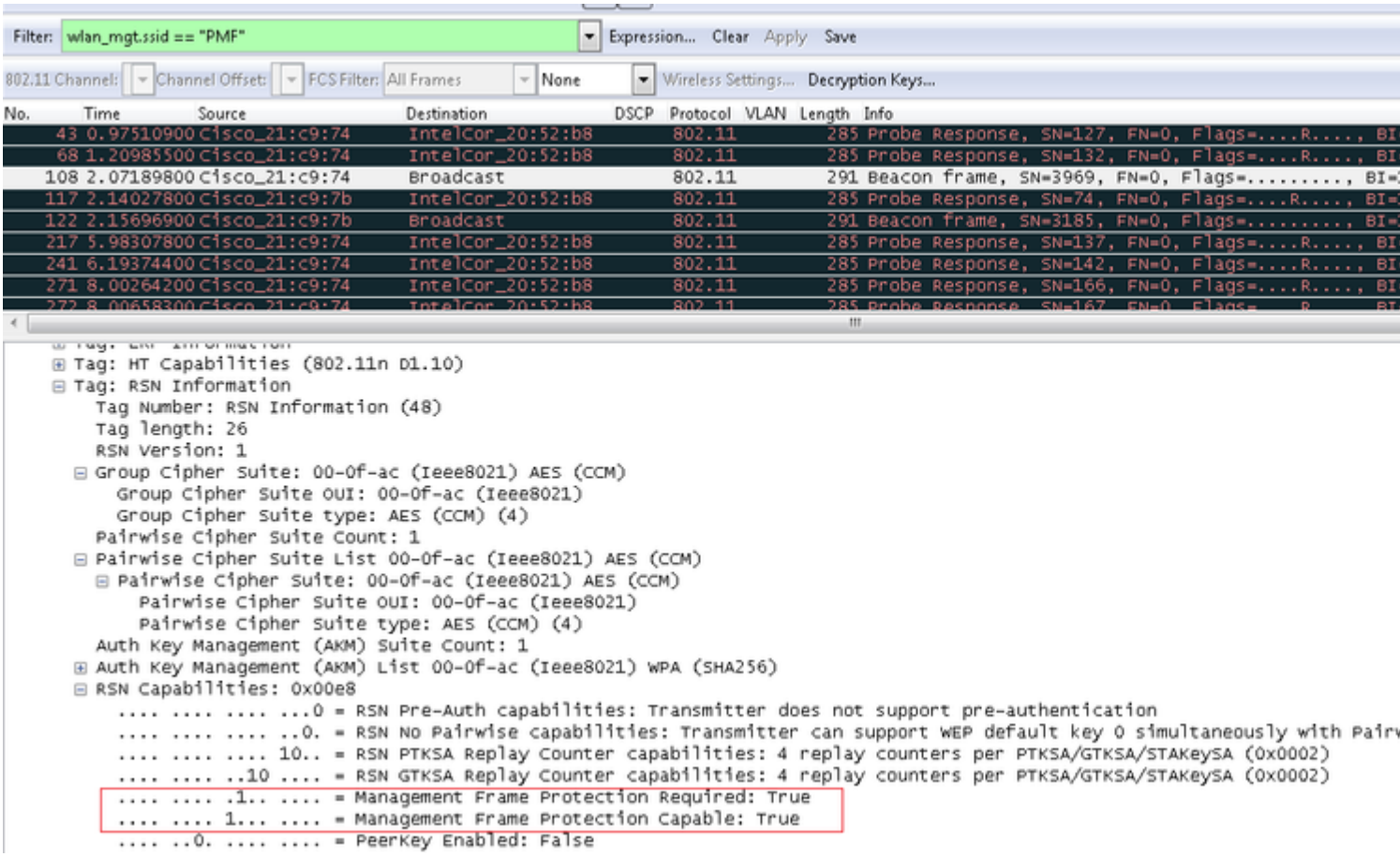


Hier vindt u het veld **van** de **groepsbeheeralgoritme** waaruit blijkt dat 802.11w wordt gebruikt.

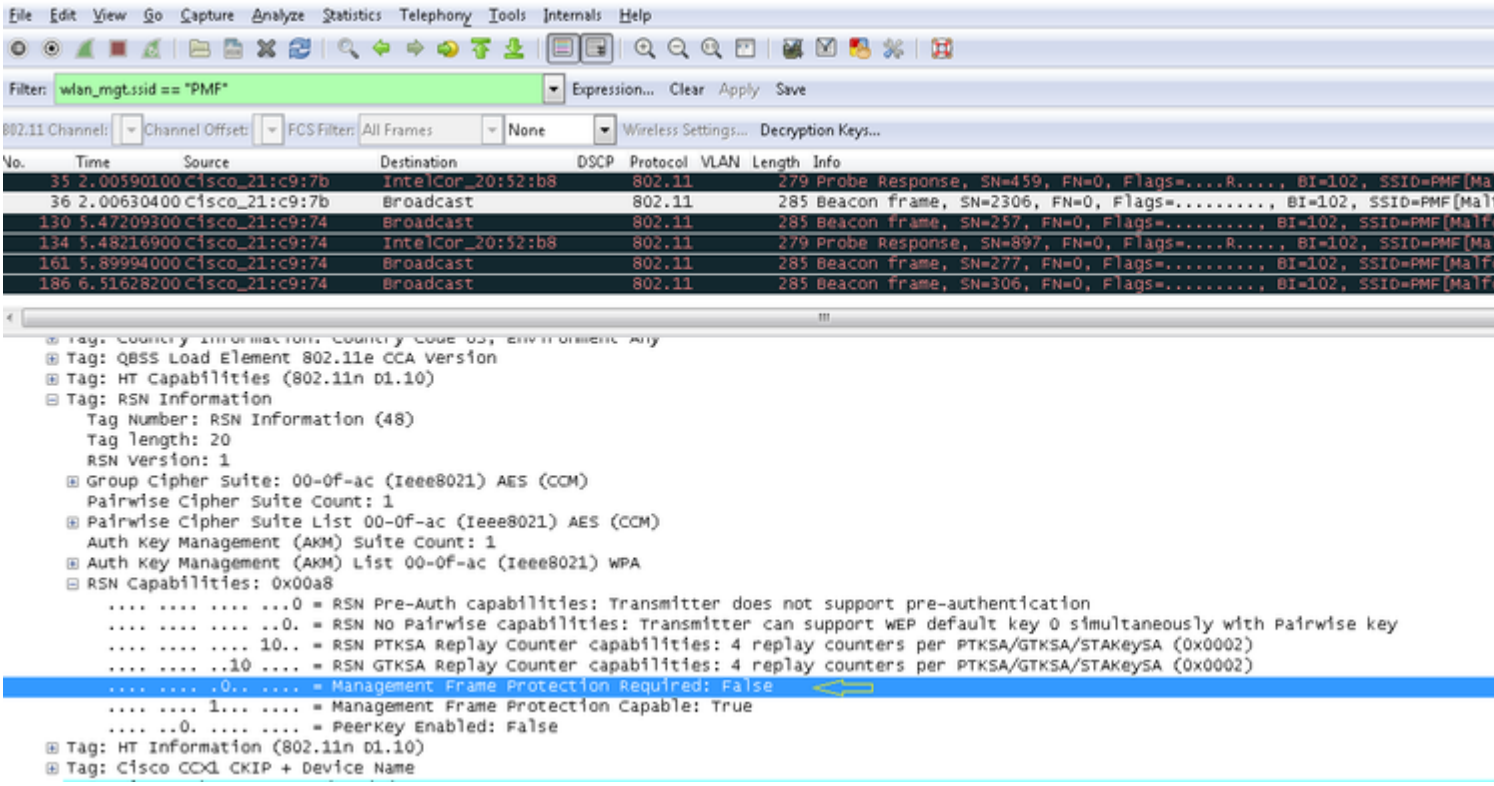
Er werden ook veranderingen doorgevoerd onder RSN-mogelijkheden. De bits 6 en 7 worden nu gebruikt om de verschillende parameters voor 802.11w aan te geven.

- Bit 6: Management Frame Protection Required (MFPR) - Een STA stelt dit bit in op 1 om te adverteren dat de bescherming van Robust Management Frames verplicht is.
- Bit 7: Management Frame Protection Capable (MFPC) - Een STA stelt dit bit in op 1 om te adverteren dat de bescherming van Robust Management Frames is ingeschakeld. Wanneer het toegangspunt dit instelt, deelt het mee dat het de bescherming van het beheerframe ondersteunt.

Als u de bescherming van het beheerskader zoals vereist onder de configuratieopties instelt, worden zowel bits 6 als 7 ingesteld. Dit is zoals hier getoond in het beeld van de pakketopname.



Als u dit echter op optioneel instelt, wordt alleen bit 7 ingesteld, zoals in de afbeelding wordt weergegeven.



Opmerking: De WLC voegt deze gewijzigde RSN IE toe in associatie/re-associatie antwoorden en de AP voegt deze gewijzigde RSN IE toe in beacons en sonde antwoorden.

Voordelen van 802.11w Management Frame Protection

- Clientbescherming

Dit wordt bereikt door cryptografische bescherming toe te voegen aan deauthenticatie- en disassociatiekaders. Dit voorkomt dat een niet-geautoriseerde gebruiker een DOS-aanval (Denial of Service) start door het MAC-adres van legitieme gebruikers te spoofen en de deauth-/disassociatiekaders te verzenden.

- AP-bescherming

De bescherming aan de infrastructuurzijde wordt toegevoegd door de toevoeging van een Security Association (SA) neerwaartse beschermingsmechanisme dat uit een Association Comeback Time en een SA-Query procedure bestaat. Vóór 802.11w, als een AP een Associatie- of Verificatieaanvraag heeft ontvangen van een reeds gekoppelde client, beëindigt de AP de huidige verbinding en start vervolgens een nieuwe verbinding. Wanneer u 802.11w MFP gebruikt, indien de STA is gekoppeld en heeft onderhandeld over Management Frame Protection, wijst de AP het Associatieverzoek met retourstatuscode 30 af Association request rejected temporarily; Try again later aan de cliënt.

In de Association Response is een Association Comeback Time informatie element dat een comeback tijd specificeert wanneer de AP klaar is om een associatie met deze STA te accepteren. Op deze manier kunt u ervoor zorgen dat legitieme klanten niet worden losgekoppeld vanwege een spoofed associatieverzoek.

> **Opmerking**: De WLC (AireOS of 9800) negeert de door de clients verzonden deconfessies of deauthenticatie frames als ze geen 802.11w PMF gebruiken. De client vermelding wordt alleen verwijderd direct na ontvangst van een dergelijk frame als de client PMF gebruikt. Dit om te voorkomen dat kwaadaardige apparaten de dienst ontzeggen, aangezien er geen beveiliging is op die frames zonder PMF.

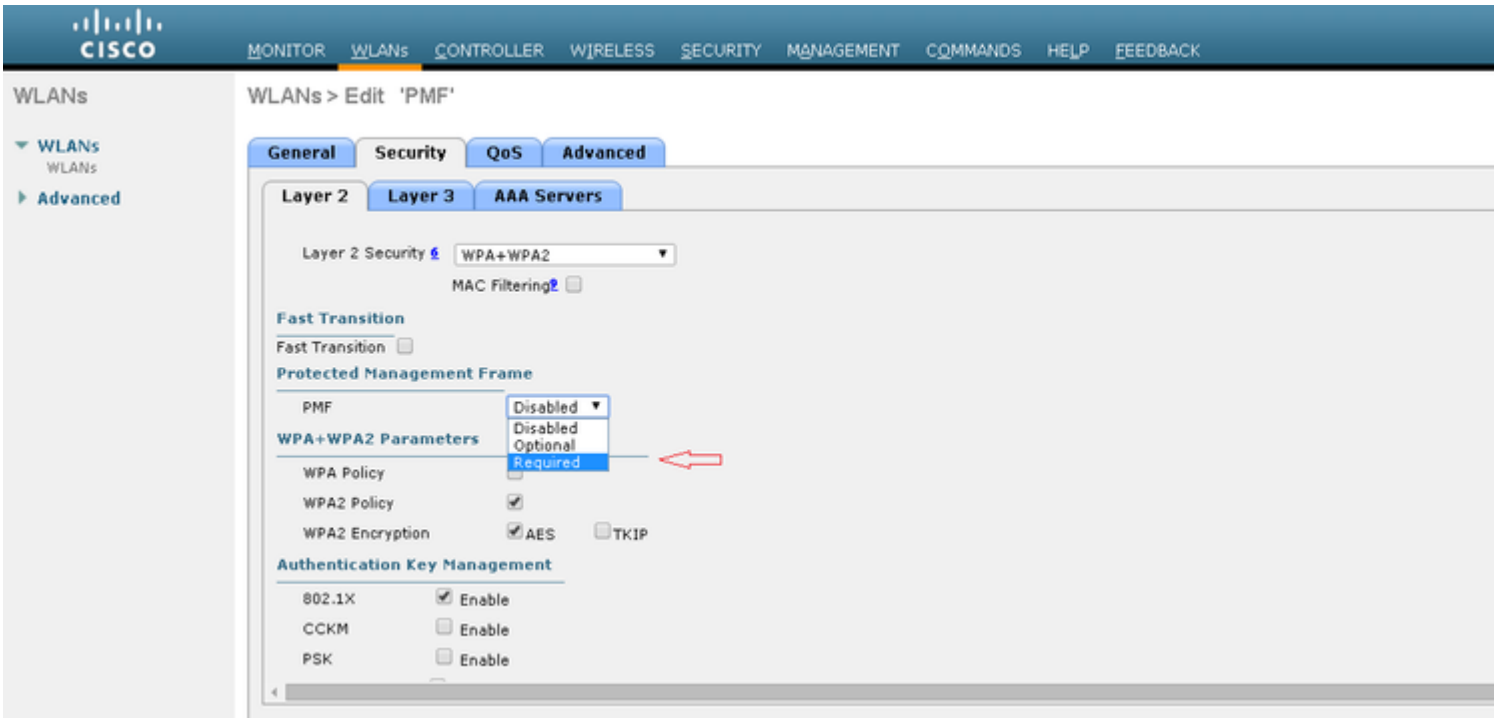
Vereisten voor het inschakelen van 802.11w

- 802.11w vereist dat de SSID wordt geconfigureerd met dot1x of PSK.
- 802.11w wordt ondersteund op alle 802.11n-compatibele AP. Dit betekent dat AP 1130 en 1240 802.11w niet ondersteunen.
- 802.11w wordt niet ondersteund op flexconnect AP en 7510 WLC in de 7.4 release. Ondersteuning is toegevoegd sinds de 7.5 release.

Configureren

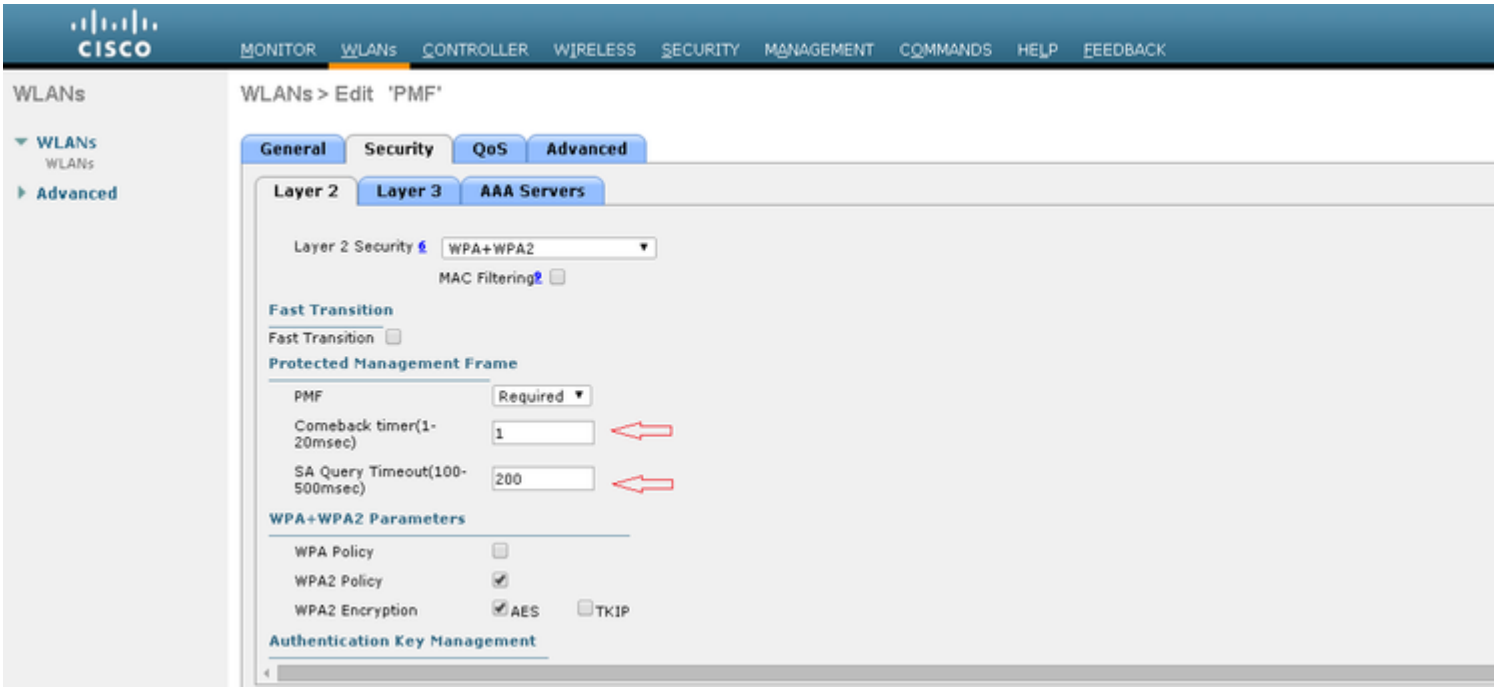
GUI

Stap 1. U moet het beveiligde beheerframe inschakelen onder de SSID die is geconfigureerd met 802.1x/PSK. U hebt drie opties zoals in de afbeelding.

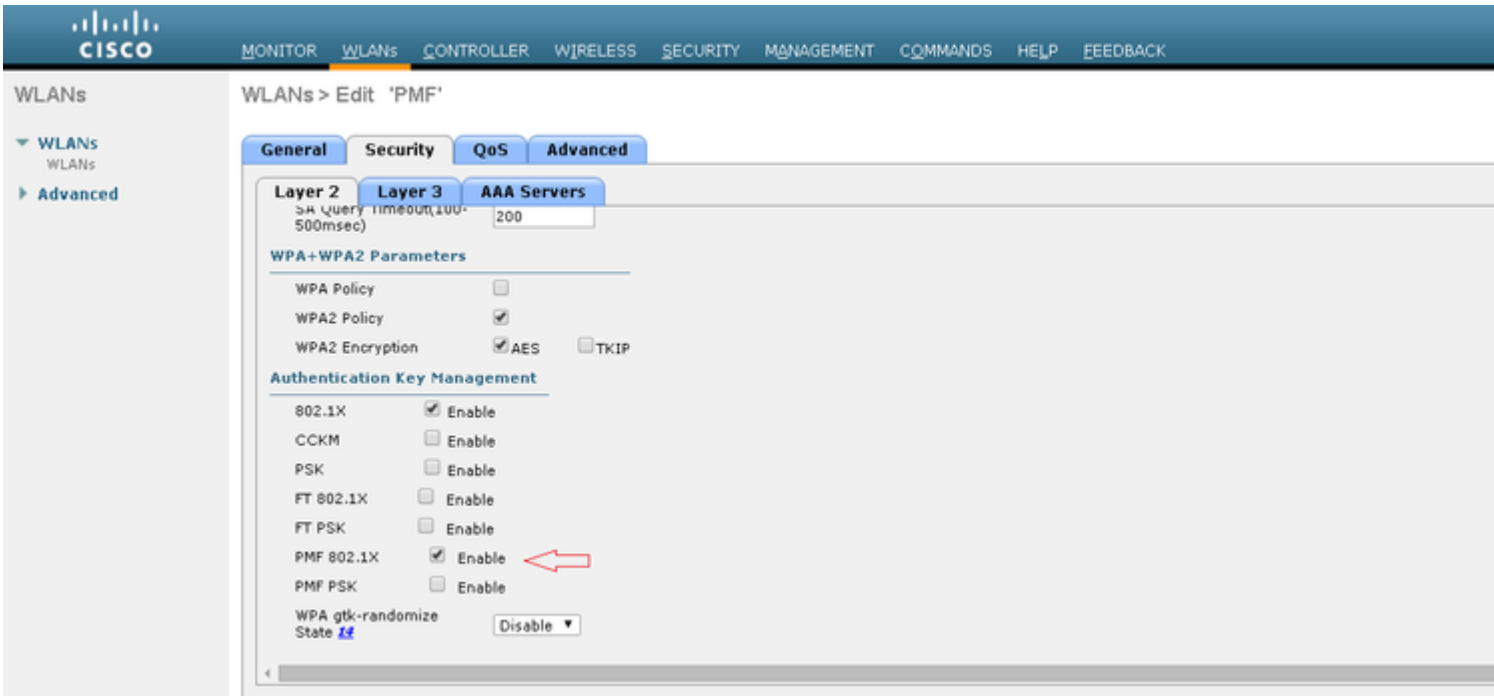


'Vereist' geeft aan dat een client die 802.11w niet ondersteunt, geen verbinding mag maken. 'Optioneel' geeft aan dat zelfs clients die 802.11w niet ondersteunen, verbinding mogen maken.

Stap 2. U moet vervolgens de comeback timer en SA query timeout opgeven. De comeback timer geeft de tijd aan dat een gekoppelde client moet wachten voordat de associatie opnieuw kan worden geprobeerd wanneer deze eerst wordt ontkend met een statuscode 30. SA query timeout specificeert de hoeveelheid tijd die de WLC wacht op een reactie van de client voor het query proces. Als de client niet reageert, wordt de associatie van de controller verwijderd. Dit gebeurt zoals in de afbeelding.



Stap 3. U moet 'PMF 802.1x' inschakelen als u 802.1x gebruikt als de verificatiesleutelbeheermethode. Als u PSK gebruikt, moet u het selectievakje **PMF PSK** kiezen zoals in de afbeelding.



CLI

- Om de 11w-functie in of uit te schakelen voert u de opdracht uit:

config wlan security wpa akm pmf 802.1x enable/disable

config wlan security wpa akm pmf psk enable/disable

- Voer de opdracht uit om beschermde beheerframes in te schakelen of uit te schakelen:

config wlan security pmf optional/required/disable

- Instellingen associatie-terugverdientijd:

config wlan security pmf 11w-association-comeback

- Instellingen voor opnieuw proberen SA-query:

config wlan security pmf saquery-retry-time

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De 802.11w-configuratie kan worden geverifieerd. Controleer de WLAN-configuratie:

```
(wlc)>show wlan 1
Wi-Fi Protected Access (WPA/WPA2)............. Enabled
<snip>
802.1x................................ Enabled
PSK................................... Disabled
CCKM.................................. Disabled
FT-1X(802.11r)........................ Disabled
FT-PSK(802.11r)....................... Disabled
PMF-1X(802.11w)....................... Enabled
PMF-PSK(802.11w)...................... Disabled
FT Reassociation Timeout.................. 20
FT Over-The-DS mode....................... Enabled
GTK Randomization......................... Disabled
<snip>
PMF.......................................... Required
PMF Association Comeback Time................. 1
PMF SA Query RetryTimeout..................... 200
```

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Deze debug commando's zijn beschikbaar om 802.11w problemen op te lossen op de WLC:

- **debug 11w-pmf events enable/disable**
- debug 11w-pmf keys enable/disable
- debug 11w-pmf all enable

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.